ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

УКРАЇНА

(19) UA **(11) 94039** **(13) U**

(51) МПК (2014.01)
G09C 1/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2014 05191**

(22) Дата подання заявки: **16.05.2014**

(24) Дата, з якої є чинними права на корисну модель: **27.10.2014**

(46) Публікація відомостей про видачу патенту: **27.10.2014, Бюл.№ 20**

(72) Винахідник(и):
Лужецький Володимир Андрійович (UA),
Баришев Юрій Володимирович (UA)

(73) Власник(и):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

(54) СПОСІБ ПАРАЛЕЛЬНОГО КЛЮЧОВОГО ГЕШУВАННЯ ДАНИХ ТЕОРЕТИЧНО ДОВЕДЕНОЇ СТІЙКОСТІ

(57) Реферат:

Спосіб паралельного ключового гешування даних теоретично доведеної стійкості включає подання інформаційних даних у вигляді послідовності. Потім подають ключові дані K, гешування інформаційних даних виконують шляхом піднесення до степеня за модулем за допомогою пристрою піднесення до степеня за модулем, задача зламу ключа гешування зводиться до обчислення дискретного логарифма в полі простого числа, підносять число, яке є примітивним коренем за модулем. Ключові дані K подають у вигляді послідовності секретних чисел, підносять кожне з q великих чисел, яке є примітивним коренем за відповідним модулем p_j, до степеня, який є результатом додавання значення елемента інформаційної послідовності m_i, значення суми результатів гешування попереднього елемента інформаційної послідовності та значення секретного числа k_j.

UA 94039 U

Корисна модель належить до галузі криптографічного захисту інформації і може бути використана при розробці механізмів забезпечення цілісності даних.

Відомий спосіб ключового хешування теоретично доведеної стійкості - [Патент України № 18693 від 15.11.2006 р., М. кл. G 09 C 1/00, бюл. № 11 2006 р.], який полягає в тому, що інформаційні дані M подаються у вигляді послідовності $M=\{m_1, m_2 \ldots m_l\}$, ключові дані K подаються у вигляді великого секретного числа k, а хешування інформаційних даних виконується за допомогою пристрою множення елементів m_i інформаційної послідовності M та елементів ключової послідовності K за ітеративним правилом піднесення до степеня за модулем великого простого числа p, ключові дані, в подальшому особистий ключ k^*, використовуються як степінь ступеня в ітераційному правилі хешування, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі.

Недоліком цього способу є недостатня теоретична стійкість внаслідок того, що для заданого значення числа p не всі значення елементів інформаційної послідовності m_i дозволяють отримати повну множину вихідних значень (від 0 до p-1) при виконанні операцій піднесення до різних степенів за модулем p, оскільки не всі значення елементів інформаційної послідовності m_i є примітивними коренями за модулем p, що робить можливим для зловмисника злам за допомогою перебору відмінного від повного, а тому задача зламу не зводиться до обчислення дискретного логарифма в полі простого числа.

Найбільш близьким до способу, що пропонується, є спосіб ключового хешування теоретично доведеної стійкості [Патент України № 50818 від 25.06.2010 р., М. кл. G 09 C 1/00, бюл. № 12, 2010 р.], який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2 \ldots m_l\}$, ключові дані K подають у вигляді великого секретного числа k, а хешування інформаційних даних виконують шляхом піднесення до степеня за модулем великого простого числа p за допомогою пристрою піднесення до степеня за модулем, велике секретне число k використовують як початкове заповнення h_0, задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі, підносять велике число g, яке є примітивним коренем за модулем p, степінь, до якого виконують піднесення, є результатом додавання значення елемента інформаційної послідовності m_i та результату хешування, в подальшому гешування, попереднього елемента інформаційної послідовності.

Недоліком найближчого аналога є недостатня обчислювальна швидкість гешування, оскільки для піднесення w-розрядного великого числа g за допомогою w-розрядного пристрою піднесення до степеня за модулем ($n=w \cdot q$, $q \geq 1$) необхідно виконати $O(q^2)$ операцій піднесення до степеня для кожного елемента інформаційної послідовності m_i.

В основу корисної моделі поставлена задача створити спосіб паралельного ключового гешування даних теоретично доведеної стійкості, який дозволить забезпечити підвищену обчислювальну швидкість гешування даних за рахунок виконання операції піднесення до степеня за допомогою q пристроїв піднесення до степеня за модулем.

Технічний результат, який може буде отриманий при здійсненні корисної моделі, полягає в підвищенні швидкості обчислення геш-значення повідомлення.

Поставлена задача вирішується за рахунок того, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2 \ldots m_l\}$, подають ключові дані K, гешування інформаційних даних виконують шляхом піднесення до степеня за модулем за допомогою пристрою піднесення до степеня за модулем, задача зламу ключа гешування зводиться до обчислення дискретного логарифма в полі простого числа, підносять число, яке є примітивним коренем за модулем, згідно з корисною моделлю, ключові дані K подають у вигляді послідовності секретних чисел $\{k_1, k_2, \ldots, k_q\}$, підносять кожне з q великих чисел g_i (j=1, 2,…, q), яке є примітивним коренем за відповідним модулем p_i, до степеня, який є результатом додавання значення елемента інформаційної послідовності m_i, значення суми результатів хешування попереднього елемента інформаційної послідовності та значення секретного числа k_i.

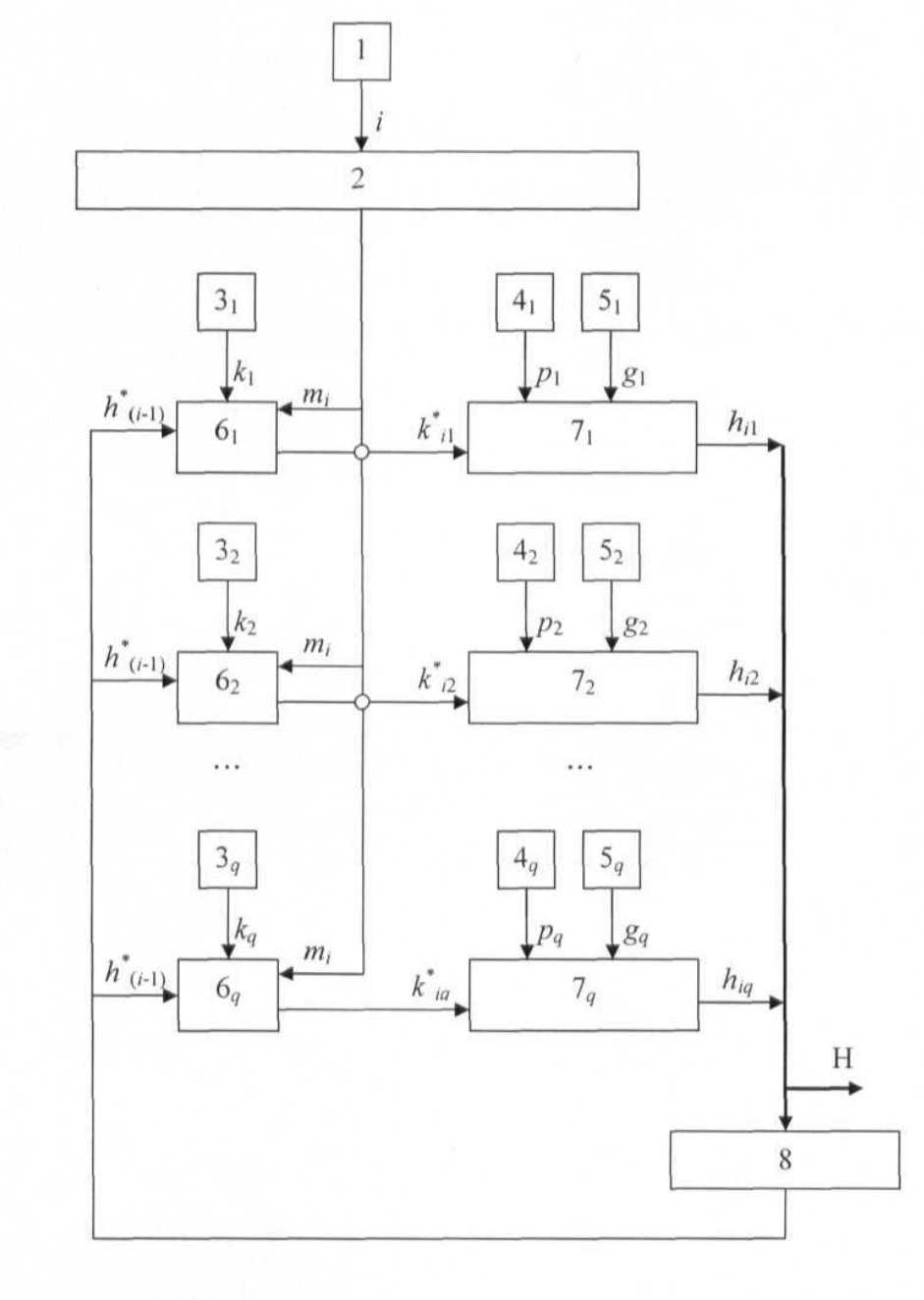
На кресленні наведена схема пристрою, що реалізує спосіб паралельного ключового гешування даних теоретично доведеної стійкості.

Пристрій містить лічильник 1 вихід, якого з'єднано з входом оперативно запам'ятовуючого пристрою 2, вихід якого є третім входом j-го пристрою додавання 6_i ($j \in N$, у є [1; q]). Першим входом j-го пристрою додавання 6_i є вихід (q+1)-го пристрою додавання 8, а другим - вихід блока зберігання j-ї частини ключа 3_i. Вихід у-го пристрою додавання 6_v з'єднано з першим входом j-го пристрою піднесення до степеня за модулем 7. Другим входом j-го пристрою піднесення до степеня за модулем 7_i є вихід блока зберігання j-го значення модуля 4_i, а третім - вихід блока зберігання j-го примітивного елемента 5_i. Вихід j-го пристрою піднесення до степеня за модулем 7_j, є j-м входом (q+1)-го пристрою додавання 8 та j-м виходом всього пристрою.

Спосіб паралельного ключового гешування даних теоретично доведеної стійкості виконується на пристрої таким чином. В блок зберігання j-ї частини ключа 3_i надсилають значення j-ї частини ключа k_i, в блок зберігання j-го значення модуля 4_i - значення j-го модуля p_i, в блок зберігання j-го примітивного елемента 5_i - значення примітивного елемента g_i за модулем p_i. В оперативно запам'ятовуючий пристрій 2 заносять інформаційні дані, що підлягають гешуванню, представлені у вигляді послідовності $\{m_1, m_2 \ldots m_l\}$, а лічильник 1 встановлюють в положення, що відповідає початковій адресі оперативно запам'ятовуючого пристрою 2, де зберігається перший елемент інформаційної послідовності m_1. Вихід (q+1)-го пристрою додавання 8 встановлюють рівним нулю. Починають ітеративний процес. З виходу лічильника 1 отримують адресу i-го елемента інформаційної послідовності m_i та надсилають її до оперативно запам'ятовуючого пристрою 2, з виходу якого отримують значення i-го елемента інформаційної послідовності m_i, яке надсилають на третій вхід j-го пристрою додавання 6_i. За допомогою j-го пристрою додавання 6_i додають значення i-го елемента інформаційної послідовності m_i, значення $h^*_{(i-1)}$, яке отримують з виходу (q+1)-го пристрою додавання 8, та значення j-ї частини ключа k_i, яке отримують з виходу блока зберігання j-ї частини ключа 3_i. Значення показника степеня k^*_{ij}, отримане з виходу j-го пристрою додавання 6_j надсилають на перший вхід j-го пристрою піднесення до степеня за модулем 7_i, де виконують піднесення значення примітивного елемента g_i за модулем p_i, отриманого з виходу блока зберігання j-го примітивного елемента 5_j, до степеня k^*_{ij}, за модулем p_j, значення якого отримують з виходу блока зберігання j-го значення модуля 4_i. Значення результату піднесення до степеня за модулем h_{ji}, отримане з виходу j-го пристрою піднесення до степеня за модулем 7_i надсилають на j-й вхід (g+1)-го пристрою додавання 8. За допомогою (g+1)-го пристрою додавання 8 додають q значень результатів піднесення до степеня. Якщо $i \neq l$, то змінюють положення лічильника 1 відповідно адреси (i+1)-го елемента інформаційної послідовності та починають наступну ітерацію, інакше зупиняють ітеративний процес. Після l-ї ітерації частину результуючого геш-значення h_{li} отриману на виході j-го пристрою піднесення до степеня за модулем 7_i надсилають на j-й вихід всього пристрою.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб паралельного ключового гешування даних теоретично доведеної стійкості, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, \ldots, m_l\}$, подають ключові дані K, гешування інформаційних даних виконують шляхом піднесення до степеня за модулем за допомогою пристрою піднесення до степеня за модулем, задача зламу ключа гешування зводиться до обчислення дискретного логарифму в полі простого числа, підносять число, яке є примітивним коренем за модулем, який **відрізняється** тим, що ключові дані K подають у вигляді послідовності секретних чисел $[k_1, k_2, \ldots, k_q]$, підносять кожне з q великих чисел g_j (j=1, 2, …, q), яке є примітивним коренем за відповідним модулем p_j, до степеня, який є результатом додавання значення елемента інформаційної послідовності m_i, значення суми результатів гешування попереднього елемента інформаційної послідовності та значення секретного числа k_j.



Комп'ютерна верстка М. Шамоніна

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601